MedEnc Technologies Inc.
2482 Yonge Street #1116,Toronto, ON M4P 2H5 Canada
https://medenc.com
https://moanr.app
info@medenc.com

Intimate Surveillance: Privacy Violations, Regulatory Gaps, and the Zero-Knowledge Paradigm in the HealthTech and FemTech Sectors — V2

A Comprehensive Whitepaper on Data Privacy, Cyber Vulnerabilities, and Cryptographic Safeguards in Consumer Digital Health

1. Executive Summary

The rapid expansion of the mobile health (mHealth) and reproductive technology (FemTech) markets has fundamentally transformed consumer wellness, with the global FemTech sector projected to reach a valuation of $50 billion by 2025 [1, 2]. However, what began as a wave of empowering, consumer-centric tools for digital self-care has, in many instances, devolved into a matrix of "intimate surveillance" [3]. This whitepaper provides an in-depth analysis of the systemic privacy and security crises plaguing modern health applications, specifically focusing on documented breaches of trust, regulatory failures under the Health Insurance Portability and Accountability Act (HIPAA), and catastrophic cybersecurity exploits. Finally, it outlines the emerging legal and technical frontiers—such as state-level health privacy statutes and MedEnc Technologies' pioneering Zero-Knowledge cryptographic paradigm—to establish a secure, trust-validated blueprint for the future of digital health.

2. The Paradigm of Intimate Surveillance and the Digital Health Revolution

Every day, millions of individuals record their most private physiological and psychological data on smartphone applications. Within the FemTech sector, platforms continuously harvest rich longitudinal datasets: menstrual cycle lengths, basal body temperatures, hormone fluctuations, symptoms of physical pain, and intimate lifestyle profiles including sexual activity and contraceptive use [1, 3]. Similarly, mental health and meditation platforms gather detailed data on users' moods, cognitive stressors, anxieties, and clinical symptoms [4, 5].

A critical gap exists between consumer expectations and industry practices. The average consumer does not read or fully comprehend lengthy, complex privacy policies, unknowingly forfeiting their data rights during simple click-to-consent onboarding [3, 6]. Most users operate under the false assumption that any application collecting biological or mental health data is automatically protected by federal confidentiality laws [6, 7]. In reality, developers frequently leverage this lack of literacy, utilizing vague terms of service to establish permissive, behind-the-scenes data-sharing practices that monetize intimate telemetry for targeted advertising, lookalike marketing, and broker sales [3, 8].

3. Regulatory Gaps and Legal Arbitrage under HIPAA

The primary health privacy law in the United States, the Health Insurance Portability and Accountability Act (HIPAA) of 1996, is widely misunderstood [6, 8]. Despite its reputation as an all-encompassing shield for medical confidentiality, HIPAA's regulatory jurisdiction is strictly limited to "covered entities"—defined as healthcare providers, health plans, healthcare clearinghouses, and their direct business associates who facilitate electronic medical billing [7, 8]. Crucially, HIPAA regulates the **entity** handling the data rather than the **class** of the data itself [7, 8].

This structural boundary creates a system of legal arbitrage: if an individual records details regarding prescription drugs, symptoms, or diagnoses into an Electronic Health Record (EHR) maintained by a licensed physician, that clinical dialogue is protected under HIPAA [7, 8]. However, if that same individual records identical information into a commercial mental health app, a smart wearable device, or a search engine query, that data falls entirely outside HIPAA's protective ambit [6, 7]. Commercial entities are legally free to store, aggregate, and distribute this health telemetry to third-party advertising technology (ad-tech) companies and data brokers, provided they do not actively deceive consumers about these practices [6, 8].

4. Landmark Case Studies: Breaches of Trust and Commercial Exploitation

In the absence of comprehensive federal health privacy standards, the Federal Trade Commission (FTC) has aggressively stepped in to govern non-HIPAA-regulated health apps [6, 7, 9]. Leveraging Section 5 of the FTC Act (which prohibits unfair or deceptive practices) and the Health Breach Notification Rule (HBNR), the FTC has prosecuted several high-profile platforms for severe breaches of trust [7, 9]:

- **BetterHelp [9, 10]:** Pushed users to complete a highly sensitive diagnostic intake questionnaire covering clinical depression and suicidal ideation, promising absolute confidentiality. In practice, the platform integrated tracking pixels and cookies from Facebook, Snapchat, Pinterest, and Criteo, systematically piping users' intake answers and social media profiles into marketing engines to run targeted lookalike advertising campaigns. The FTC imposed a $7.8 million settlement for consumer redress.
- **GoodRx [8, 9]:** A telehealth and prescription drug discount platform that promised users HIPAA-like security and displayed deceptive compliance seals. Instead, GoodRx utilized tracking pixels to transfer consumers' precise prescription drug names, dosages, and underlying medical conditions to third-party ad networks. GoodRx paid a $1.5 million civil penalty in the FTC’s first-ever enforcement action under the Health Breach Notification Rule (HBNR).
- **Premom (Easy Healthcare Corporation) [9, 11]:** Easy Healthcare explicitly promised that Premom's reproductive health data would never be shared without consent. In reality, the app integrated third-party Software Development Kits (SDKs) from Google, AppsFlyer, and Chinese-headquartered firms Umeng and Jiguang (JPush). These integrations transmitted unencrypted Custom App Events (such as *LogFertility* and *Guarantee/signup*) over the network. Furthermore, the Jiguang SDK bypassed operating system privacy controls, exploiting a known Android vulnerability to aggressively harvest non-resettable hardware identifiers (Wi-Fi MAC addresses, IMEI numbers, and router SSIDs) to build permanent, real-world identity profiles linked to reproductive behaviors. Premom faced a major FTC penalty and a lifetime ban on sharing health data for advertising.
- **Flo Health [1, 9]:** Despite explicit promises to protect user data, Flo utilized software development kits to systematically share the daily menstruation schedules, contraceptive habits, and pregnancy statuses of over 200 million users directly with marketing analytics platforms like Facebook and Google, triggering ongoing state-level class-action litigations.
- **IQVIA Operations France [12, 13]:** In a landmark European case, the French data protection authority (CNIL) issued a €5 million administrative fine against IQVIA in May 2026. IQVIA argued that the longitudinal clinical data of tens of millions of patients aggregated in its LRX and EMR data warehouses was fully "anonymous" and exempt from GDPR. The CNIL firmly rejected this defense, ruling that the data was merely "pseudonymous" due to the presence of a unique patient identifier, the sheer depth of the clinical histories, and the ease of re-identifying individuals by combining IQVIA's tables with public data. The CNIL cited severe security failures,

including the lack of multi-factor authentication (MFA) to access the EMR warehouse, the failure to regularly analyze connection logs, and a critical system flaw where pharmacy software continued to transmit data to IQVIA even after patients had explicitly objected (Article 25 "Privacy by Design" violation).

The table below provides a structured comparative summary of these landmark enforcement actions and their underlying technical exfiltration vectors:

App / Company	Sectors & Data Type	Core Exposure Mechanism	Legal & Financial Penalties
BetterHelp [9, 10]	Mental Health; Diagnostic intake answers	Transmission of depression and suicidal ideation metrics to Facebook, Criteo, Snapchat, and Pinterest via tracking pixels.	$7.8 Million consumer redress settlement; permanent ban on health data sharing for advertising; forced downstream deletion.
GoodRx [8, 9]	Telehealth & Pharmacy; Prescription drug names and dosages	Systematic transfer of prescription drug logs and dosages to third-party ad networks; deceptive HIPAA-compliance claims.	$1.5 Million civil penalty; permanent advertising ban using sensitive health data; first-ever Health Breach Notification Rule (HBNR) penalty.
Premom [9, 11]	FemTech; Ovulation schedules, physical location, and hardware IDs	Unencrypted "Custom App Events" via Google/AppsFlyer SDKs; Jiguang JPush SDK bypassed Android OS restrictions to harvest MAC addresses and SSIDs.	$200,000 in federal and state civil penalties; lifetime ban on sharing reproductive health data for advertising; mandatory downstream audit.
IQVIA France [12, 13]	Health Data Warehouses; Longitudinal pharmacy and clinical records	Treatment of pseudonymous datasets as anonymous; lack of MFA and weak connection log analysis; software transmitted data despite active user objections.	€5 Million administrative fine (CNIL, May 2026); six-month compliance mandate subject to a €10,000 daily penalty for delay.

5. Catastrophic Cybersecurity Breaches: The Cyber Frontier

While the deceptive commercialization of health data represents a calculated business decision, digital health platforms remain vulnerable to catastrophic, hostile cyber-attacks [3]. These incidents demonstrate that a failure to implement robust cybersecurity standards is functionally equivalent to a deliberate privacy violation, exposing consumers to severe stigma, distress, and fraud [3, 14].

The late 2022 ransomware attack on Medibank Private, one of Australia's largest health insurers, represents a highly severe case study in the weaponization of stolen medical telemetry [14, 15]. The breach impacted approximately 9.7 million current and former customers, exposing personal medical histories, government Medicare numbers, and passport details [14, 16]. The attack vector was traced back to a critical security failure: an employee of a contracted third-party IT provider saved their Medibank administrative credentials to a personal internet browser profile on their work computer [15]. These credentials synced to their personal device, which was subsequently compromised by info-stealing malware [15].

Using these stolen credentials, the threat actor authenticated onto Medibank's corporate Virtual Private Network (VPN) [15]. Crucially, Medibank’s VPN gateway did not require multi-factor authentication (MFA); it relied strictly on single-factor username and password validation paired with a device certificate [15]. Once inside the corporate network, the attacker installed malicious scripts and quietly exfiltrated approximately 520 gigabytes of sensitive data over a period of several weeks [15]. Although Medibank's automated Endpoint Detection and Response (EDR) security software repeatedly generated high-severity alerts regarding suspicious data volumes, the IT Security Operations team failed to appropriately triage or escalate these notifications, allowing the attacker to complete the theft undetected [15].

Following Medibank's refusal to pay a US $10 million ransom demand, the Russian-linked ransomware syndicate REvil began systematically publishing the stolen medical claims on a dark web blog [14, 16]. In an effort to maximize psychological leverage and public humiliation, the hackers separated the data into a "good list" and a "naughty list" [16]. The "naughty list" specifically targeted individuals who had received clinical treatment for drug addiction, alcohol abuse, and mental health conditions [16]. Subsequently, the attackers posted a highly specialized, unencrypted file explicitly labeled "abortions," which exposed the full reproductive histories, service provider codes, and hospital locations of thousands of female customers [16]. The Medibank cyber-attack demonstrates that health data privacy is a critical security issue; without robust controls like MFA, continuous EDR triage, and zero-trust network segmentation, highly sensitive health profiles will remain prime targets for hostile nation-states and global ransomware syndicates [3, 15].

6. The Post-Roe Legal Crisis and Domain-Specific Implications

The overturning of Roe v. Wade in the summer of 2022 profoundly shifted the risk landscape for digital health privacy in the United States [1, 3, 17]. Prior to this ruling, the unauthorized monetization of reproductive telemetry was primarily viewed as an invasive commercial nuisance [3]. Post-2022, however, the collection of menstrual cycles, ovulation patterns, contraceptive uses, and physical location data has emerged as a high-stakes legal vulnerability, with the potential to criminalize individuals seeking abortions, managing miscarriages, or experiencing pregnancy loss [1, 3, 17].

In jurisdictions where reproductive healthcare is restricted or criminalized, digital footprints can serve as a key forensic

database for law enforcement agencies and hostile civil litigants [3, 17]. A state prosecutor, armed with a subpoena or utilizing commercially purchased data-broker records, can easily reconstruct an individual's private reproductive journey [3, 17]. By analyzing the sudden cessation of period tracking on a mobile app, geofencing coordinates that indicate physical visits to out-of-state healthcare facilities, and mobile browser searches for reproductive medications, state actors can build highly detailed circumstantial cases to support criminal prosecution [1, 3, 17].

This vulnerability is exacerbated by the extensive data-sharing provisions embedded in standard commercial privacy policies [17]. Industry-wide audits indicate that approximately 67% of period-tracking applications explicitly state in their privacy agreements that they will share sensitive user data to fulfill "legal obligations" [17]. Because these policies are notoriously complex, consumers often unwittingly forfeit their constitutional privacy protections [3, 6]. Furthermore, digital tracking data remains vulnerable to exploitation by ideological groups [3]. For example, the anti-abortion organization known as The Veritas Society utilized commercially acquired location data from mobile ad networks to identify individuals visiting Planned Parenthood clinics in Wisconsin, subsequently targeting those specific devices with digital harassment and misinformation campaigns [3].

In response to these heightened anxieties, the German-based period-tracking application Clue has heavily marketed its European incorporation as a shield against US judicial overreach [18, 19, 20]. Because Clue is headquartered in Berlin, all user data is stored within the European Union and is strictly governed by the General Data Protection Regulation (GDPR) [18, 20]. GDPR provides a significantly more robust baseline of consumer protections compared to US frameworks, establishing health data as a "special category" requiring explicit, unambiguous opt-in consent [2, 20]. Clue's executive leadership has formally stated that the company will not comply with foreign US subpoenas or court orders demanding access to user reproductive records, asserting that assisting in an abortion-related prosecution would directly violate European data privacy principles [18, 19, 20]. Clue maintains that any attempt by a US authority to execute a mutual legal assistance treaty to access German servers would be vigorously contested in German courts [18, 19, 20]. However, even within GDPR-compliant platforms, absolute privacy remains elusive [18, 20]. Mozilla's independent evaluation highlighted that Clue's default architecture still engages in opt-out data sharing with ad networks for marketing optimization, requiring users to manually navigate complex settings to achieve true data isolation [18, 20]. This dynamic underscores the persistent tension between standard ad-tech monetization strategies and the rigorous demands of absolute reproductive privacy [18, 20].

7. Emerging Legislative Frontiers: WA MHMDA and KCDPA

To combat the HIPAA loophole and protect non-regulated consumer health data, states are establishing sweeping legislative frameworks:

- **Washington My Health My Data Act (MHMDA) [21, 22]:** Enacted in April 2023, MHMDA represents the most rigorous consumer health privacy statute in the United States. It defines "consumer health data" expansively to include any personal information linkable to a consumer's physical or mental health status, including biometric, genetic, and precise location coordinates indicating attempts to receive healthcare [21, 22]. Crucially, the act implements a near-absolute ban on geofencing within 2,000 feet of healthcare facilities and provides a powerful **Private Right of Action** under the Washington Consumer Protection Act [21, 22]. This allows private citizens to file civil lawsuits directly against non-compliant entities, creating immense class-action risks for tech developers [21].
- **Kentucky Consumer Data Privacy Act (KCDPA) [7, 23]:** Effective January 1, 2026, the KCDPA extends

privacy obligations far beyond HIPAA-covered entities, mandating clear privacy notices and prior opt-in consent before processing any "sensitive data" (which includes all non-HIPAA consumer-generated health information) of Kentucky residents [7].

8. Architectural Mitigations: The Zero-Knowledge Paradigm

Standard cloud-storage systems typically utilize architectures where server-side keys are managed in the cloud or pure client-side raw block storage is enforced (severely limiting high-performance search indexing, relational matching, and sharing workflows) [24]. To bridge this divide, next-generation platforms like MedEnc Technologies (Moanr™) have patented a secure, **Zero-Knowledge Cloud Backend**. This architecture executes on-the-fly database transactions using client-supplied symmetric keys without ever persistently storing or caching the keys on server disks or log repositories [24]:

1. **Ephemeral Key Processing Loop [24]:** During a database transaction, the client transmits an unencrypted payload (protected in transit by TLS 1.3) alongside a mathematically derived, symmetric AES-256 key in a custom HTTP request header (*X-medenc-key*). The backend server loads the key directly into volatile, short-lived execution memory (RAM). Once the cryptographic operation completes, the backend actively overwrites the backing byte array with zero values (0x00) using java.util.Arrays.fill(). The key is never cached, logged, or written to disk, rendering subpoenas and backend database breaches technically impossible to fulfill or exploit.
2. **Shadow UUID Decoupling [24]:** The authentication database and metrics database are strictly isolated. Authenticating user IDs (UIDs) are mapped to randomized, independent Shadow UUIDs using a cryptographically secure one-way hash. The transaction database remains completely blind, containing only encrypted blobs categorized under randomized Shadow UUID hashes, preventing cross-collection correlation attacks.
3. **Deterministic Chronological Date Offsetting [24]:** To prevent traffic correlation and timeline-matching attacks, the server retrieves a user-specific random offset (*dateOffSet*) from the encrypted user settings, applying it deterministically:
   `Offset Date = Date + dateOffSet`
   This preserves the relative chronological order for range queries while completely masking real-world timestamps from backend administrative access.
4. **Tripartite Encrypted Keybox [24]:** When partners establish a secure connection, their mutual sharing parameters are governed by three isolated records: a personal partner record for User A (encrypted with User A's master key), a personal partner record for User B (encrypted with User B's master key), and an independent Shared Link Document (Keybox) encrypted with a connection-level symmetric key. Neither partner's master key is ever exposed to the other, and the server remains blind to the sharing permissions.

To clarify the structural differences, the table below contrasts Traditional Cloud Database systems with MedEnc's Zero-Knowledge Architecture across primary privacy vectors:

Privacy Vector	Traditional Wellness Applications	Zero-Knowledge Cryptographic Paradigm [24, 25]
Data Accessibility	Plaintext databases are accessible to developers, marketing trackers, database administrators, and cloud hosts [3, 23].	Payloads are unreadable to all third parties. Decryption keys are held strictly by local devices or ephemeral memory.
Impact of Database Breach	Severe: direct leak of sensitive physical, mental, and reproductive records on public and dark web forums [14, 16].	Zero: threat actors acquire only blind, scrambled, encrypted blobs that are mathematically impossible to decrypt.
Response to Subpoenas	Servers decrypt and yield complete user medical histories and geographical logs to legal authorities [3, 17].	Subpoenas are technically impossible to fulfill. The server hosts blind blobs; the server does not hold the keys to decrypt.
Ad-Tech Integration	Intimate telemetry and mood swings are sold to data brokers and ad networks to run highly targeted marketing [3, 9, 23].	System design renders behavioral profiling impossible. No tracking pixels, marketing SDKs, or background exfiltration.

9. Actionable Policy and Operational Recommendations

To restore consumer trust, close the non-HIPAA regulatory gap, and navigate overlapping data privacy laws, we propose the following strategic framework [3, 7, 21]:

For Digital Health and FemTech Application Developers [3]:

- **Adhere to Privacy-by-Design (GDPR Article 25) [12]:** Developers must implement opt-in data collection by default. Banners must provide equal prominence to "accept" and "reject" selections, and a user's choice to opt-out must immediately update the code stack, blocking all downstream tracking [13, 26].
- **Conduct Continuous SDK Auditing [11]:** The integration of third-party analytics and ad SDKs (such as Google, Facebook, or Jiguang) must be strictly controlled, monitored, and audited to prevent the silent, unencrypted harvesting of sensitive custom events and non-resettable hardware IDs.
- **Enforce Data Minimization and Clean Deletion [3, 23]:** Organizations must actively minimize data collection, gathering only the records necessary for the application's primary functions. When a user deletes their profile or uninstalls the app, all records must be permanently and immediately purged from active, backup, and archive systems, rather than retained for three years under vague administrative terms.

For Healthcare Providers and Clinical Systems [7]:

- **Map Patient Data Flows:** As patient-generated health data (PGHD) from wearables and consumer applications is increasingly integrated into clinical workflows, providers must meticulously map data flows to identify where HIPAA or state statutes (such as KCDPA and MHMDA) apply.
- **Perform Vendor Compliance Due Diligence:** Before clinical integration, healthcare administrators must review third-party app contracts, verifying vendor compliance, validating data-encryption standards, and ensuring strict Business Associate Agreements (BAAs) are executed where appropriate.

For State and Federal Legislators [3, 21]:

- **Pass Comprehensive Sectoral Privacy Laws:** Legislators must propose comprehensive data privacy standards that explicitly cover and protect non-HIPAA-regulated health, reproductive, and biometric data. These laws should incorporate stringent geofencing prohibitions, mandatory audit requirements, and robust civil penalties.
- **Integrate a Private Right of Action:** To ensure effective enforcement, state-level regulations should follow Washington State's MHMDA blueprint, incorporating private rights of action to empower individuals and protect vulnerable populations against predatory commercial exploitation [21, 22].

10. References

1. Saini, S., & Saxena, N. (2024). Privacy and Security of Women's Reproductive Health Apps in a Changing Legal Landscape. *arXiv preprint arXiv:2404.05876*.
2. Cao, J., Laabadli, H., Mathis, C., Stern, R., & Emami-Naeini, P. (2024). “I Deleted It After the Overturn of Roe v. Wade”: Understanding Women’s Privacy Concerns Toward Period-Tracking Apps in the Post Roe v. Wade Era. *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '24)*.
3. Sherry, M. (2025). Privacy Implications of FemTech Post-Roe. *Ford School of Science, Technology, and Public Policy, University of Michigan*.
4. Caltrider, J., Rykov, M., & MacDonald, Z. (2023). Are mental health apps better or worse for privacy in 2023? *Mozilla Foundation, Privacy Not Included Guide*.
5. Park, E., & West, D. M. (2023). Why mental health apps need to take privacy more seriously. *Brookings Institution, Center for Technology Innovation*.
6. Addonizio, G. (2023). The Privacy Risks Surrounding Consumer Health and Fitness Apps with HIPAA’s Limitations and the FTC’s Guidance. *Seton Hall Law School*.
7. Michael, V. (2025). Beyond HIPAA: Legal Risks of Consumer Health Apps and Wearables for Kentucky Healthcare Providers. *McBrayer PLLC, Healthcare Law Blog*.
8. Sherman, J. (2023). GoodRx, Health Data Brokerage, and the Limits of HIPAA. *Lawfare Media, Cybersecurity & Tech*.
9. Jillson, E. (2023). Protecting the Privacy of Health Information: A Baker's Dozen of Takeaways from FTC Cases. *NYU Law School Program on Corporate Compliance and Enforcement*.
10. Frankfurt Kurnit Klein & Selz PC (2023). FTC, OCR, and HHS Issue Warning Letter Concerning Use of Online Tracking Technologies. *Technology Law Blog*.
11. Sherman, J. (2023). The FTC, Fertility App Premom, and Sharing Consumer Health Data. *Lawfare Media, Surveillance & Privacy*.
12. Commission Nationale de l'Informatique et des Libertés (CNIL) (2026). Health data: fine of 5 million euros against

IQVIA Operations France. *CNIL, Decisions of the Restricted Committee (SAN-2026-008)*.
13. Dooley, S. (2026). CNIL fines IQVIA €5m over health data warehouse breaches. *Measured Collective, EU Enforcement Cases*.
14. Prictor, M. (2023). Data Breach Notification Laws—Momentum Across the Asia-Pacific Region: The Medibank Private Incident. *Journal of Bioethical Inquiry, Springer*.
15. Office of the Australian Information Commissioner (OAIC) (2023). Medibank data breach: alleged timeline. *OAIC Federal Court Concise Statement Filings*.
16. Taylor, J. (2022). Medibank hacker says ransom demand was US$10m as purported abortion health records posted. *The Guardian (Australia)*.
17. Edgerton, K. F., Compton, L. D., & Stewart, K. (2023). OCR and FTC Issue Joint Statement Warning Health Care Providers and App Developers About Use of Third Party Online Tracking Technologies. *Mintz Levin, Digital Health Advisory*.
18. Mozilla Foundation (2022). Clue Period & Cycle Tracker: Privacy & Security Guide. *Mozilla Foundation, Privacy Not Included*.
19. Clue Support (2025). What is Clue's stance on data privacy? *BioWink GmbH Help Center*.
20. Shea, A. (2025). Big data research on women's health with Clue. *BioWink GmbH Science & Research Library*.
21. Washington State Office of the Attorney General (2023). Protecting Washingtonians' Personal Health Data and Privacy: My Health My Data Act (HB 1155). *AG Consumer Protection Divisions*.
22. Perkins Coie LLP (2023). My Health My Data Act (MHMD): Navigating Washington State's Health Privacy Law. *Perkins Coie, Privacy & Security Guidance*.
23. Newmark, W. (2025). Data brokers and data privacy: Monetization, regulation, and how they affect consumers. *Usercentrics Global Privacy Insights*.
24. MedEnc Technologies, Inc. (2026). System and Method for Secure, Privacy-Preserving Zero-Knowledge Database Synchronization. *US Patent Application / Plain English Privacy Guide (zeroKnowledgePatent.pdf)*.
25. MedEnc Technologies, Inc. (2026). Moanr™ Core Feature Catalog & Architectural Specifications. *MedEnc Product Systems Directory (features.pdf)*.
26. UniConsent Team (2026). GDPR Enforcement and Fines 2026: Business Categories, Top Cases, and Country. *UniConsent Ad Tech and Publisher Compliance Reports*.